

REMARKS

Summary of Claim Status

Claims 1-20 are pending in the present application after entry of the present amendment. Claims 1-8 and 14-20 are rejected for the reasons discussed below.

Claims 9-13 are allowed. Applicants thank the Examiner for this acknowledgement of patentable subject matter.

Applicants respectfully request entry of the present amendments, which are believed to place the application in condition for allowance, and further respectfully request favorable reconsideration of the claims and withdrawal of the pending rejections and objections in view of the present amendment and in light of the following discussion.

Rejections Under 35 U.S.C. § 103

Claims 1-5, 14, 16, and 17 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Trimberger, U.S. Patent No. 5,892,961 ("Trimberger"), in view of Erickson, U.S. Patent No. 5,970,142 ("Erickson"). Applicants respectfully disagree, and submit that Trimberger and Erickson, alone or in any combination, do not teach or even suggest the claimed inventions. However, the rejection is believed to be moot in light of the present amendment.

Applicants have amended Claim 1 to recite a plurality of data words specifying a design, wherein a subset of a plurality of unencrypted words for controlling loading of configuration data indicates whether the plurality of data words specifying the design is a plurality of encrypted words specifying an encrypted design. The amendment is fully supported by the specification as filed, for example at page 14, lines 20-26, of the specification.

Applicants respectfully submit that Trimberger and Erickson, alone or in any combination, do not teach or even suggest the invention of amended Claim 1. In particular, neither Trimberger nor Erickson teaches unencrypted control words that indicate whether a plurality of data words specifying the design is a plurality of encrypted words for specifying an encrypted design. In fact, Erickson teaches away from such an invention since "the PLD 110 generates the pseudo-random

key 180 each time it is programmed, and the key 180 is used to encrypt the configuration data 130.” Erickson at col. 3, lines 42-45. That is, in Erickson a key is generated each time a PLD is programmed, and there is no option to leave the data unencrypted, and thus there would be no need for control words to indicate whether data words specifying the design are encrypted words.

In contrast, Claim 1 recites that “a subset of the plurality of unencrypted words for controlling loading of configuration data indicates whether the plurality of data words specifying the design is a plurality of encrypted words specifying an encrypted design.” As noted in the specification, there are occasions for which it is preferable not to encrypt the bitstream, such as during testing and debugging, or when multiple designers are writing code.

Therefore, Applicants respectfully request entry of the amendment and allowance of Claim 1.

Claims 2-5, 14, 16, and 17 depend from Claim 1, and thus include all of the limitations of Claim 1. Applicants believe Claim 1 is allowable for the reasons set forth above. Therefore, for at least the same reasons, Applicants believe Claims 2-5, 14, 16, and 17 are also allowable, and allowance of such claims is respectfully requested.

Claims 6-8 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Trimberger, in view of Erickson, and further in view of Kwiat, U.S. Patent No. 5,931,959 (“Kwiat”). Applicants respectfully disagree, and submit that Trimberger, Erickson, and Kwiat, alone or in any combination, do not teach or even suggest the claimed inventions. However, the rejection is believed to be moot in light of the present amendments. In particular, Claims 6-8 depend from Claim 1, and thus include all of the limitations of Claim 1. Applicants believe Claim 1 is allowable for the reasons set forth above. Therefore, for at least the same reasons, Applicants believe Claims 6-8 are also allowable, and respectfully request allowance of Claims 6-8.

Claim 15 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Trimberger, in view of Erickson, and further in view of Yin, U.S. Patent No.

6,028,939 ("Yin"). Applicants respectfully disagree, and submit that Trimberger, Erickson, and Yin, alone or in any combination, do not teach or even suggest the claimed invention. However, the rejection is believed to be moot in light of the present amendments. In particular, Claim 15 depends from Claim 1, and thus includes all of the limitations of Claim 1. Applicants believe Claim 1 is allowable for the reasons set forth above. Therefore, for at least the same reasons, Applicants believe Claim 15 is also allowable, and respectfully request allowance of Claim 15.

Claims 18-20 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Trimberger, in view of Erickson, and further in view of Yin. Applicants respectfully disagree, and submit that Trimberger, Erickson, and Yin, alone or in any combination, do not teach or even suggest the claimed inventions.

In the response to Applicants' arguments, the Examiner stated that Yin discloses a step of forming a cipher block chaining initial value comprising a starting address for loading a design into a PLD. In particular, the Office Action stated: "the 64 bit initial vector IV which is shown on figure 2b, ref. Num. '42', is starting address for loading a design or predetermined sequence of bits into a PHE or PLD as explained on column 7, lines 60-65 and column 8, lines 59-67." Applicants respectfully disagree with this characterization of the reference.

First, the cited sections of Yin do not appear to teach that reference number 42 is a starting address for loading a design into a PLD as recited in Claim 18. As described in Yin, reference number 42 is merely a 64-bit initial vector (IV) used to produce a cipher block. Yin at col. 5, lines 39-40. There is no suggestion in Yin that the initial vector 42 is any kind of address, much less a starting address for loading a design into a PLD.

Moreover, it is clear that the PHE (programmable hardware element) 114 in Yin, which may be a PLD, is used as a peripheral for the integrated hardware/software data security system 100 of Yin. See, e.g., Yin at col. 7, line 30 – col. 9, line 30. As described in Yin, the PHE 114 may be used for a variety of functions, including to control the microprocessor to provide a compatible data rate (col. 7, lines 51-54), to perform communications network functions such as IP

checksums (col. 7, line 58-60), to act as an extension of the processor (col. 8, lines 15-17), to be configured to take advantage of a bursting mode (col. 8, lines 23-26), and to accelerate portions of the symmetric block encryption process and perform hashing and random number generation (col. 8, lines 31-37). Thus, in Yin the PHE is merely an additional processing element used to provide acceleration to the security system described in Yin. As noted in Yin, it may be advantageous to perform certain hardware functions in the PHE, and allocate software functions to the processor, in order to achieve significantly higher performance. Yin at col. 9, lines 40-50.

In stark contrast to Yin, Claim 18 recites a method for generating a bitstream with encrypted design data. Nowhere in Yin is a bitstream for a design even mentioned, much less taught or suggested. Furthermore, it is clear that the system described in Yin requires the combination of a PHE with a microprocessor to enable the “cost effective, scaleable and high performance” implementation noted by the Examiner at Yin, col. 5, lines 6-8. Thus, the alleged motivation is inapplicable to Claim 18.

As is well-established, *prima facie* obviousness requires that all of the claim limitations are taught or suggested by the prior art. See, e.g., MPEP § 2143.03. Neither Erickson nor Yin teaches the limitations in Claim 18 of forming a cipher block chaining initial value comprising a starting address for loading a design into a PLD, and combining the cipher block chaining initial value with a first word of design data to form a first combined word. In particular, there is no teaching or suggestion in either Erickson or Yin that an address and words of design data may be combined in this manner to form a combined word. If the rejection is to be maintained, Applicants respectfully request that the Examiner point out the specific sections of Erickson or Yin that teach these limitations.

For at least the foregoing reasons, Applicants believe Claim 18 is allowable, and allowance of Claim 18 is respectfully requested.

Claims 19 and 20 depend from Claim 18, and thus include all of the limitations of Claim 18. Applicants believe Claim 18 is allowable for the reasons set forth above. Therefore, for at least the same reasons, Applicants believe

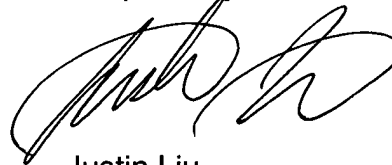
Claims 19 and 20 are also allowable, and allowance of such claims is respectfully requested.

Conclusion

Applicants acknowledge an unusually thorough and helpful analysis of all pending claims by the Examiner.

No new matter has been introduced by any of the above amendments. Applicants request that the Examiner reconsider the final rejection and consider the above arguments and amendments. These arguments and amendments are believed to clearly indicate that the application including Claims 1-20 should be allowed. Therefore, Applicants respectfully request allowance of the application. If any action other than allowance is contemplated by the Examiner, the Examiner is invited to telephone Applicants' attorney at 408-879-4641.

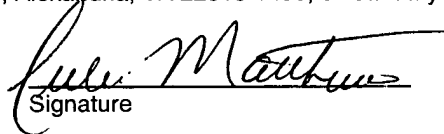
Respectfully submitted,



Justin Liu
Attorney for Applicants
Reg. No. 51,959

I hereby certify that this correspondence is being deposited with the United States Postal Service as first-class mail in an envelope addressed to: Commissioner for Patents, P.O. BOX 1450, Alexandria, VA 22313-1450, on January 16, 2006.

Julie Matthews
Name


Signature